多天线主动窃听系统的干扰机优化设计 *

涂小岚 [1]，张广驰 [1]，万林青 [1]，崔　苗 [1]，林　凡 [2]

(1. 广东工业大学, 信息工程学院, 广州 510006; 2. 广州杰赛科技股份有限公司, 广州 510310)

摘　要：不同于与传统无线通信物理层安全被动窃听技术，针对物理层主动窃听技术进行了研究，主要用于合法部门监听可疑用户的通信。考虑可疑发射机和合法干扰机具有多天线、可疑接收机和合法窃听者具有单天线的系统模型，在可疑通信链路增益强于窃听链路增益的情况下，通过发射干扰信号，控制可疑用户的通信速率，使合法窃听者能正确解码窃听信息。分别在合法干扰机对合法窃听者有/无干扰的两种情况下，进行最优的干扰信号设计和干扰功率控制，最大化窃听速率。仿真结果表明，在不同的应用场景下合理设置干扰机位置，能有效提高窃听速率，并且所提的干扰机设计方法均取得了比现有的两种基准方法更优的窃听性能。

关键词：主动窃听；干扰信号设计；干扰功率控制；窃听速率性能

中图分类号：TN918.91　　doi: 10.3969/j.issn.1001-3695.2017.07.0694

Jammer optimization for multi-antenna proactive eavesdropping systems

Tu Xiaolan[1], Zhang Guangchi[1], Wan Linqing[1], Cui Miao[1], Lin Fan[2]

(1. *School of Information Engineering Guangdong University of Technology*, *Guangzhou* 510006, *China*); 2. *Guangzhou GCI Science & Technology Co*, *Ltd*, *Guangzhou* 510310, *China*)

Abstract: Different with the passive wireless eavesdropping technique in traditional wireless communications, this paper studied proactive eavesdropping technology at the physical layer for legitimate eavesdropper to monitor the communication between suspicious users. It equipped consider a multiple-input single-output (MISO) system model where the suspicious transmitter and legitimate jammer with multi antennas, and equipped the suspicious receiver and legitimate eavesdropper with single antenna, If the channel gain of the suspicious communication link was stronger than that of the eavesdropping link, the legitimate jammer controls the communication rate of the suspicious users via jamming them, in order for the legitimate eavesdropper to correctly decode the eavesdropped information. Considering two cases that the jammer could or culdn't interference on the legitimate eavesdropper, respectively, it designed the optimal interference signal and power control for the legitimate jammer to maximize the eavesdropping rate. Simulation results show that the proposed interference design method for the jammer in different application scenarios has achieved better eavesdropping performance than the existing two benchmark methods.

Key Words: proactive eavesdropping; jamming signal design; interference power control; eavesdropping rate performance

0　引言

无线通信技术的迅速发展，在为人们带来便利的同时也带来了隐私、秘密信息泄露的风险。

保障信息的安全传输[1~3]，一直是信息安全[1]当中的一项重要研究内容。在无线网络中，无线通信利用本身的广播传输特性，一方面能够给授权用户之间提供便利的信息传输通道，但这也容易被不法分子利用，试图发动恶意攻击，意图盗取用户身份信息、密码信息等。上述恶意攻击行为被称为被动窃听攻击。被动窃听者通常只是被动的窃听用户的信息，但是不会主动攻击接收者接受信息。应对此类物理层安全事件的防被动窃听技术有：

a）传统的密码加密技术[2]。传统的加密机制通过有效的技术来加密信息，以确保对窃听的拦截；虽然这项技术在安全通信方面提供了有效的防范方法，但是随着窃听者群体的快速膨胀扩大，增加密钥和管理的复杂度也是传统机制目前需要面临

基金项目：国家自然科学基金资金项目（61571138）；广东省自然科学基金资金项目（2015A030313481）；广东省学科建设专项资金科技创新项目（2013KJCX0060）；广东省科技计划项目（2016A050503044，2016KZ010101，2016KZ010107，2016KZ010101，2016B090904001，2014B090901061，2015B090901060，2015B090908001）；广州市科技计划项目（201710010082，201604020127，2014Y2-00211）；广东工业大学培英育才计划项目（220411321）

作者简介：涂小岚（1992-），女（通信作者），湖北人，硕士研究生，主要研究方向为无线通信系统（840482142@qq.com）；张广驰（1982-），男，广东人，副教授，博士，主要研究方向为宽带无线通信系统、协作通信技术等；万林青（1993-），女，江西人，学生，研究生，主要研究方向为无线通信系统；崔苗，女，新疆人，讲师，博士，主要研究方向为宽带无线通信系统；林凡，男，高级工程师，研究生，主要研究方向为宽带无线通信系统.

的巨大挑战。

b）物理层安全方式[4]~[6]。利用信号传输的信道及噪声特性，通过恶化窃听者信道环境进而提高物理层信息传输的安全性。目前这项安全防护技术，具有广阔的应用前景和应用价值。

通常情况下考虑窃听是非法行为，然而实际上窃听者可以发动主动攻击来增强他们的窃听性能，这被称为主动窃听[7]-[10]。在特种安全领域，主动窃听是侦查犯罪分子和恐怖分子等可疑用户通信的过程，目的是为了减少犯法行为的发生。政府机构窃听可疑无线通信的行为被认为是合法的。

目前，学术界提出的主要物理层主动窃听技术有两种：a) 基于干扰的主动窃听技术[7]。合法窃听者距离可疑传输机较远的情况下，其中全双工的合法窃听者通过发射干扰信号，在实现窃听的同时调整可疑通信速率，目的是为了加强窃听效果。

b)窃听者作为中继转发干扰信号的主动窃听技术。窃听者作为一个中继[8] [9]，在窃听信道较好的情况下，放大转发一个有利信号到接收机；相反的情况下，转发一个破坏信号。通过迷惑源发射机，使得窃听者可以顺利解码窃听信息。

然而在文献[7～10]中,仅考虑的是单天线的应用场景，针对实际应用场景，考虑单独增加一个多天线干扰机；在可移动范围内，调整干扰机的发射功率；干扰机距离可疑接收机较近时，系统的窃听性能越强，有效设置干扰机的位置，

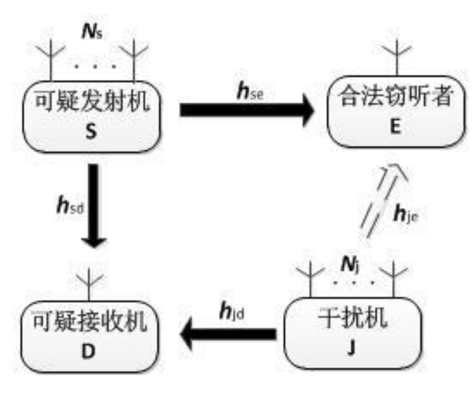


图 1　主动窃听系统模型

能够提高系统的合法窃听性能。因此在文献[7]所提出的基于干扰的主动窃听技术的基础上，考虑在一个多输入单输出(multiple-input single-output，MISO)多天线模型中，增加一个多天线干扰机，通过优化干扰机的发射功率，提高系统的窃听速率；其中窃听者作为窃听方，基于文献[7]对于主动窃听的定义：在衰落信道下，当窃听速率大于可疑通信速率的时候，合法窃听者能够成功解码、窃听可疑通信链路。分别在有自干扰（合法窃听者自身受到干扰机干扰）和无自干扰（由于采用了干扰消除技术，合法窃听者不受干扰机干扰）两种情况下，多天线干扰机根据自适应功率调整方案，发射干扰信号干扰接收机的信号接收。窃听速率越大，表示系统窃听信道状态越强，因此针对提高系统性能，主要集中优化的是合法窃听速率，并且分别利用内点法[11~13]和拉格朗日优化方法[11,14]优化干扰机的发射功率，最大限度地提高系统合法窃听速率。通过计算机仿真验证，与已有的两种基准干扰策略相比，所提的干扰信号优化方案，取得了更优的窃听速率性能。

符号：粗体小写、大写字母分别表示向量和矩阵，$\boldsymbol{Z}^{\mathrm{T}}$，$\boldsymbol{Z}^{\mathrm{H}}$ 表示矩阵的转置、共轭转置，$\mathrm{trace}(\boldsymbol{Z})$ 表示矩阵的迹。$\|\boldsymbol{Z}\|$ 为矩阵 Z 的范数，$\|z\|$ 为向量 z 的欧几里德范数（2 范数）。

1　系统模型

考虑在多输入单输出-MISO 瑞利衰落信道下的一个合法无线监测场景（图 1）；其中合法窃听者负责监控点对点可疑通信链路，在窃听环境弱于通信环境时，干扰机发射干扰信号，干扰可疑用户之间的通信。N_s、N_j 分别为可疑发射机 S、干扰机 J 的天线数；可疑接收机 D、合法窃听者 E 均考虑的是单天线设备；$\boldsymbol{h}_{sd}$、$\boldsymbol{h}_{se}$、$\boldsymbol{h}_{jd}$、$\boldsymbol{h}_{je}$ 分别为可疑发射机 S 到可疑接收机 D、可疑发射机 S 到合法窃听者 E、干扰机到可疑接收机 D、干扰机到合法窃听者 E 之间的信道增益，且 $\boldsymbol{h}_{sd}$、$\boldsymbol{h}_{se}$、$\boldsymbol{h}_{jd}$、$\boldsymbol{h}_{je}$ 的元素服从复高斯分布，在每一帧的传输过程中均保持不变。

1.1　无主动窃听时，可疑用户的通信模型

在无主动窃听的情况下，可疑接收机 D 的接收信号为

$$\hat{y} = \sqrt{P_s} h_{sd} w x_s + n_d \tag{1}$$

其中：P_s 是可疑发射机的发射功率；$w \in \mathbb{C}^{N_s \times 1}$ 和 x_s 分别是可疑发射机的加权传输向量、发射信号，且有 $\mathbf{E}\left[x_s^2\right]=1$；$n_d \sim \mathrm{N}\left(0,\sigma^2\right)$ 为可疑接收机 D 产生的高斯白噪声。通过式(1)，给定信道下可疑接收机的平均输出信噪比为

$$\hat{r} = \frac{P_s\left|\boldsymbol{h}_{sd}\boldsymbol{w}\right|^2}{\sigma^2} \tag{2}$$

其中：发射权向量 w 的设计应使式(2)最大，通过 Schwartz 不等式，有

$$\hat{r} = \frac{P_s\left|\boldsymbol{h}_{sd}\boldsymbol{w}\right|^2}{\sigma^2} = \frac{P_s\left|\left(\boldsymbol{h}_{sd}^{\mathrm{H}},\boldsymbol{w}\right)\right|^2}{\sigma^2} \le \frac{P_s\left\|\boldsymbol{h}_{sd}^{\mathrm{H}}\right\|^2\left\|\boldsymbol{w}\right\|^2}{\sigma^2} \tag{3}$$

其中为 $\left(\boldsymbol{h}_{sd}^{\mathrm{H}},\boldsymbol{w}\right)$ 内积运算，当

$$\boldsymbol{w} = \frac{\boldsymbol{h}_{sd}^{\mathrm{H}}}{\left\|\boldsymbol{h}_{sd}^{\mathrm{H}}\right\|} \tag{4}$$

时，式(3)取等。这也是基于最大比合并发射原理[15]得出的结论，在发射端通过最大比合并原理设计加权值，最大化系统的通信速率。

1.2　主动窃听模型

假设合法窃听者 E 监控可疑发射机 S 的发射信号。在窃听监控的同时，通过干扰机 N_j 根天线发射干扰信号干扰可疑链路之间的通信[16]。干扰功率 $P_j = \mathrm{trace}\{V\}$，其中 $\boldsymbol{V} = \mathrm{E}\{\boldsymbol{v}\boldsymbol{v}^{\mathrm{H}}\}$ 为干扰信号的自相关矩阵。

合法窃听者 E、可疑接收机 D 的接收信号分别表示为

$$y_d = \sqrt{P_s}\boldsymbol{h}_{sd}\boldsymbol{w}x_s + \boldsymbol{h}_{jd}\boldsymbol{v} + n_d \tag{5}$$

$$y_e = \sqrt{P_s}\boldsymbol{h}_{se}\boldsymbol{w}x_s + a\boldsymbol{h}_{je}\boldsymbol{v} + n_e \tag{6}$$

其中：$n_e \sim \mathrm{N}(0,\sigma^2)$ 是合法窃听者 E 产生的高斯白噪声。$0 \le a \le 1$ 即为干扰指数，若 $a=0$，窃听者可以完全消除干扰信号给自身带来的影响；若 $a=1$，窃听者本身也会受到干扰信号的影响。在接下来的第 2 章,也会将两种情况分别进行分析，不同情况下的设计方案也会有所不同。

通过式(5)(6)分别得出可疑接收机 D、合法窃听者 E 的信噪比（signal-to-noise ratio，SNR）为

$$\gamma_d = \frac{P_S|\boldsymbol{h}_{sd}\boldsymbol{w}|^2}{|\boldsymbol{h}_{jd}\boldsymbol{v}|^2+\sigma^2} = \frac{P_S\left|\boldsymbol{h}_{sd}\frac{\boldsymbol{h}_{sd}^{\mathrm{H}}}{\|\boldsymbol{h}_{sd}^{\mathrm{H}}\|}\right|^2}{|\boldsymbol{h}_{jd}\boldsymbol{v}|^2+\sigma^2} \tag{7}$$

$$\gamma_e = \frac{P_s|\boldsymbol{h}_{se}\boldsymbol{w}|^2}{a|\boldsymbol{h}_{je}\boldsymbol{v}|^2+\sigma^2} = \frac{P_S\left|\boldsymbol{h}_{se}\frac{\boldsymbol{h}_{sd}^{\mathrm{H}}}{\boldsymbol{h}_{sd}^{\mathrm{H}}}\right|^2}{a|\boldsymbol{h}_{jd}\boldsymbol{v}|^2+\sigma^2} \tag{8}$$

2 最优干扰设计

根据文献[4]，窃听信道增益大于可疑通信信道增益即 $|\boldsymbol{h}_{se}|^2 \ge |\boldsymbol{h}_{sd}|^2$，这也意味着窃听者的信道增益较强，窃听者可以解码可疑发射机 S 的发射信号，信息泄露率即窃听速率为接收机的通信速率 $R_D=\log_2(1+r_d)$。其他情况下，窃听者不能解码窃听信号，此时的窃听速率为 0。因此窃听速率可定义为

$$\mathrm{R}_{leak} = \begin{cases} R_D \;, & 如|\boldsymbol{h}_{se}|^2 \ge |\boldsymbol{h}_{sd}|^2 \\ 0 \;, & 其他。\end{cases} \tag{9}$$

针对提高整体系统的性能，在有干扰功率约束的情况下，优化干扰信号的自相关矩阵,最大化窃听速率。基于式(9)对主动窃听的定义，最优干扰设计问题可以表述为

$$\mathrm{P}:\quad \max \quad r_d \tag{9a}$$

$$s.t \quad r_e \ge r_d \tag{9b}$$

$$\boldsymbol{V} = \boldsymbol{V}^{\mathrm{H}}, \boldsymbol{V} \ge 0 \tag{9c}$$

$$\mathrm{trace}(\boldsymbol{V}) \le Q_j \tag{9d}$$

式(9b)(9c)(9d)分别为系统的约束条件，式(9c)保证干扰信号的自相关矩阵 $\boldsymbol{V}$ 为正定矩阵，式 9d）为干扰功率下限，式(9b）即根据文献[7]中对于主动窃听的定义：合法窃听者信道状态强于可疑接收机时，合法窃听者 E 能成功解码可疑传输信号。整个系统的最终目的是优化干扰发射功率 P_j，最大化窃听速率 r_d。如果 r_d 较大,代表窃听信道状态更强。

2.1 无自干扰-基于半定规划的最优干扰信号设计.

假设整个信道状态信息是确定的，合法窃听者 E 能通过先进的模拟和数字自干扰消除方法而免于干扰信号 $\boldsymbol{v}$ 的影响。在这种情况下，窃听者的目标是优化干扰机传输功率 P_j，最大化系统窃听速率 r_d，进而提高窃听性能。

基于文献[8]对于主动窃听的定义，在满足约束条件式（9b）情况下：$\dfrac{\left|\boldsymbol{h}_{se}\frac{\boldsymbol{h}_{sd}^{\mathrm{H}}}{\boldsymbol{h}_{sd}^{\mathrm{H}}}\right|^2}{\sigma^2} \ge \dfrac{\left|\boldsymbol{h}_{sd}\frac{\boldsymbol{h}_{sd}^{\mathrm{H}}}{\|\boldsymbol{h}_{sd}^{\mathrm{H}}\|}\right|^2}{|\boldsymbol{h}_{jd}\boldsymbol{v}|^2+\sigma^2}$，问题即可解。其中干扰机采用自适应功率调整策略：窃听信道增益优于通信信道增益即 $|\boldsymbol{h}_{se}|^2 \ge |\boldsymbol{h}_{sd}|^2$，不需要干扰机的干扰也能达到主动窃听的性能，此时不考虑使用干扰机有 $P_j=0$；其他情况下的窃听判决条件为 R_r：

$$\mathrm{R}_r:\quad \max \quad \mathrm{trace}\left(\boldsymbol{h}_{jd}\boldsymbol{h}_{jd}^{\mathrm{H}}\boldsymbol{V}\right) \tag{10}$$

$$s.t \quad \boldsymbol{V} \ge 0 \tag{11}$$

$$\mathrm{trace}(\boldsymbol{V}) \le Q_j \tag{12}$$

Q_j 为此时满足判决条件下的最优功率解。根据判决条件 R_r,在通信信道增益较强 $|\boldsymbol{h}_{sd}|^2 > |\boldsymbol{h}_{se}|^2$ 时,若满足 $\dfrac{|\boldsymbol{h}_{se}\boldsymbol{w}|^2}{\sigma^2} \ge \dfrac{|\boldsymbol{h}_{sd}\boldsymbol{w}|^2}{\beta Q_j + \sigma^2}$,其中 $\beta = \mathrm{trace}(\boldsymbol{h}_{jd}\boldsymbol{h}_{jd}^{\mathrm{H}})$。

根据文献[11～13]提供的半定规划（semidefinite programming,SDP）方法，可将 P_1 转变为半定规划问题：

$$\mathrm{P}_1:\ \min \ \mathrm{trace}(\boldsymbol{A}\boldsymbol{V}_1)$$

$$s.t \quad \mathrm{trace}(\boldsymbol{A}\boldsymbol{V}_1) \ge \sigma^2\left(\frac{\boldsymbol{h}_{sd}\frac{\boldsymbol{h}_{sd}^{\mathrm{H}}}{\|\boldsymbol{h}_{sd}^{\mathrm{H}}\|}}{\boldsymbol{h}_{se}\frac{\boldsymbol{h}_{sd}^{\mathrm{H}}}{\|\boldsymbol{h}_{sd}^{\mathrm{H}}\|}} - 1\right) \tag{13}$$

$$\mathrm{trace}(\boldsymbol{V}_1) \ge 0 \tag{14}$$

$$\mathrm{trace}(\boldsymbol{V}_1) \le Q_j \tag{15}$$

其中：$A = \boldsymbol{h}_{jd}\boldsymbol{h}_{jd}^{\mathrm{H}}$、$\boldsymbol{V}_1 = \boldsymbol{v}_1\boldsymbol{v}_1^{\mathrm{H}}$。由与约束条件式（14）（15）均满足凸条件，直接利用内点法即可求解出 $\hat{\mathrm{p}}_1$ 的最优解。根据 SDP 方法优化 $\boldsymbol{v}_1$ 的自相关矩阵 $\boldsymbol{V}_1$，有且仅有最大窃听速率 $\gamma_{d1}^{\max}$：

$$\gamma_{d1}^{\max} = \frac{P_S\left|\boldsymbol{h}_{sd}\frac{\boldsymbol{h}_{sd}^{\mathrm{H}}}{\boldsymbol{h}_{sd}^{\mathrm{H}}}\right|^2}{\boldsymbol{h}_{jd}\boldsymbol{V}_1\boldsymbol{h}_{jd}^{\mathrm{H}}+\sigma^2} \tag{16}$$

2.2 2.2 自干扰条件下的干扰信号设计

$|\boldsymbol{h}_{sd}|^2 < |\boldsymbol{h}_{se}|^2$ 即窃听信道增益相对较强的时候，不发射干扰信号即 $P_j = 0$。根据式(10)，自干扰情况下需满足的窃听判决条件即为

$$\frac{\left|\boldsymbol{h}_{se}\frac{\boldsymbol{h}_{sd}^{\mathrm{H}}}{\boldsymbol{h}_{sd}^{\mathrm{H}}}\right|^2}{\left|\boldsymbol{h}_{sd}\frac{\boldsymbol{h}_{sd}^{\mathrm{H}}}{\boldsymbol{h}_{sd}^{\mathrm{H}}}\right|^2} \ge \frac{\beta_1 Q_j + \sigma^2}{\beta_2 Q_j + \sigma^2}$$

其中: $\beta_1 = \mathrm{trace}\left(\boldsymbol{h}_{je}\boldsymbol{h}_{je}^{\mathrm{H}}\right)$，$\beta_2 = \mathrm{trace}\left(\boldsymbol{h}_{jd}\boldsymbol{h}_{jd}^{\mathrm{H}}\right)$。

为了获得优化问题 P_1 在自干扰情况下的全局最优解，引用文献[11，14]中所提出的拉格朗日方法,对问题 P_1 优化求解。首先，问题 P_1 的拉格朗日原问题如下所示：

$$P_2: \min \left|\boldsymbol{h}_{jd}\boldsymbol{v}\right|^2$$

$$s.t \quad \frac{\left|\boldsymbol{h}_{je}\boldsymbol{v}\right|^2+\sigma^2}{\left|\boldsymbol{h}_{jd}\boldsymbol{v}\right|^2+\sigma^2} \le B \tag{17}$$

其中：$B=\dfrac{\left|\boldsymbol{h}_{se}\dfrac{\boldsymbol{h}_{sd}^{H}}{\boldsymbol{h}_{sd}^{H}}\right|^2}{\left|\boldsymbol{h}_{sd}\dfrac{\boldsymbol{h}_{sd}^{H}}{\boldsymbol{h}_{sd}^{H}}\right|^2}$。

引入拉格朗日对偶变量 λ，有且仅有 $\lambda\ge 0$ 满足

$$L(\boldsymbol{v},\lambda)=\left|\boldsymbol{h}_{jd}\boldsymbol{v}\right|^2-\lambda\left(B\left(\left|\boldsymbol{h}_{jd}\boldsymbol{v}\right|^2+\sigma^2\right)-\left(\left|\boldsymbol{h}_{je}\boldsymbol{v}\right|^2+\sigma^2\right)\right)=$$

$$\lambda(1-B)\sigma^2+\boldsymbol{v}\left((1-\lambda B)\boldsymbol{h}_{jd}\boldsymbol{h}_{jd}^{H}+\lambda\boldsymbol{h}_{je}\boldsymbol{h}_{je}^{H}\right)\boldsymbol{v}^{H} \tag{18}$$

对偶函数为 $g_1(\lambda)=\min\ L(\boldsymbol{v},\lambda)$。

若 $(1-\lambda B)\boldsymbol{h}_{jd}\boldsymbol{h}_{jd}^{H}+\lambda\boldsymbol{h}_{je}\boldsymbol{h}_{je}^{H}<0$，则有对偶函数 $g_1(\lambda)$ 无下界限。因此将其转换为对偶问题 $\flat$：

$$\flat \quad \max\ \lambda(1-B)\sigma^2$$

$$s.t \quad (1-\lambda B)\boldsymbol{h}_{jd}\boldsymbol{h}_{jd}^{H}+\lambda\boldsymbol{h}_{je}\boldsymbol{h}_{je}^{H}\ge 0 \tag{19}$$

由于问题 $\flat$ 为凸 SDP 问题，它的最优解可以通过内点法[11]优化方法直接求解。假设 λ^* 为 $\flat$ 的最优解。

根据文献[10]中对非凸二次约束二次规划（quadratic constrained quadratic programming，QCQP）问题的定义与其中的定义 2 可知：若有 λ^* 使 $L(\boldsymbol{v},\lambda^*)$ 为凸问题，则有 $\lambda^* f(\boldsymbol{v}^*)=0$，其 $f(\boldsymbol{v}^*)\le 0$。

因此有 $\boldsymbol{v}^*\in\min L(\boldsymbol{v},\lambda^*)$ 使得

$$\lambda^*\left((B-1)\sigma^2+B\left|\boldsymbol{h}_{jd}\boldsymbol{v}^*\right|^2-\left|\boldsymbol{h}_{je}\boldsymbol{v}^*\right|^2\right)=0 \tag{20}$$

由问题 $\flat$ 可知 $\lambda\ne 0$，可得出

$$(B-1)\sigma^2+B\times\mathrm{trace}\left(aa\times\boldsymbol{V}^*\right)-\mathrm{trace}\left(bb\times\boldsymbol{V}^*\right)=0 \tag{21}$$

经由一系列的等式变换，根据拉格朗日方法，干扰机最优发射功率 $P_j^{'}=\mathrm{trace}(\boldsymbol{V}^*)=\dfrac{(1-B)\sigma^2}{B\times aa-bb}$，其中：$aa=\boldsymbol{h}_{jd}\boldsymbol{h}_{jd}^{H}$，$bb=\boldsymbol{h}_{je}\boldsymbol{h}_{je}^{H}$，$\boldsymbol{V}^*=\boldsymbol{v}^*\boldsymbol{v}^*$。

在自干扰情况下系统最大窃听速率即为

$$\gamma_{d2}^{\max}=\frac{P_S\left|\boldsymbol{h}_{sd}\dfrac{\boldsymbol{h}_{sd}^{H}}{\boldsymbol{h}_{sd}^{H}}\right|^2}{\boldsymbol{h}_{jd}\boldsymbol{V}^*\boldsymbol{h}_{jd}^{H}+\sigma^2}$$

算法 1　自干扰/无自干扰情况下自相关矩阵 V 的优化设计

步骤 1：判断窃听信道增益与可疑通信信道增益大小关系，如 $\left|\boldsymbol{h}_{sd}\right|^2<\left|\boldsymbol{h}_{se}\right|^2$，则执行步骤 3。其他情况，则执行步骤 2，分别在无自干扰/有自干扰情况下，优化自相关矩阵 V。

步骤 2：

①无自干扰（$a=0$）：由窃听判决条件 R_r，有且仅在满足 $\dfrac{\left|\boldsymbol{h}_{se}\boldsymbol{w}\right|^2}{\sigma^2}\ge\dfrac{\left|\boldsymbol{h}_{sd}\boldsymbol{w}\right|^2}{\beta Q_j+\sigma^2}$ 时，执行半正定规划方法。根据优化问题 P_1，干扰机最优功率设计为：$P_j=\boldsymbol{V}_1$。

②自干扰（$a=1$）：由窃听判决条件 R_r，有且仅在满足 $\dfrac{\left|\boldsymbol{h}_{se}\dfrac{\boldsymbol{h}_{sd}^{H}}{\boldsymbol{h}_{sd}^{H}}\right|^2}{\left|\boldsymbol{h}_{sd}\dfrac{\boldsymbol{h}_{sd}^{H}}{\boldsymbol{h}_{sd}^{H}}\right|^2}\ge\dfrac{\beta_1 Q_j+\sigma^2}{\beta_2 Q_j+\sigma^2}$ 时，执行拉格朗日方法。根据优化问题 P_2，干扰机最优功率设计为：$P_j=\boldsymbol{V}^*$。

由此转至步骤 4，求解系统的窃听速率。

步骤 3：干扰功率 $P_j=0$。由此转到步骤 4，求解系统的窃听速率。

步骤 4：系统的窃听速率：$\gamma_d=\dfrac{P_S\left|\boldsymbol{h}_{sd}\dfrac{\boldsymbol{h}_{sd}^{H}}{\boldsymbol{h}_{sd}^{H}}\right|^2}{P_j\boldsymbol{h}_{jd}\boldsymbol{h}_{jd}^{H}+\sigma^2}$

3　仿真结果

在本章中,针对提出具有自干扰、无自干扰情况下的主动窃听方案使用计算机仿真来验证。将所提出的自适应功率调整方案与已有的两种方法进行比对，目前已有的两种基本方法分别是：

a）无干扰机的主动窃听方法。

b）有干扰机-干扰功率设为 Q_j，基于波束成形技术下采用最大比传输（maximum ratio transmission）设计干扰机的主动窃听方案。多天线干扰机利用波束成形技术，在发射端对数据先加权再发送，通过形成窄的发射波束，将能量对准目标用户，提高目标用户的解调信噪比。利用 MRT 最大比合并原理即相同的环境下，利用 MISO 系统的空间分集，多天线干扰机的加权因子利用最大比合并原理，通过在发射机添加发射权向量处理，发射机加权值：$\boldsymbol{v}=\dfrac{\boldsymbol{h}_{jd}^{H}}{\boldsymbol{h}_{jd}^{H}}$。将 Q_j 即干扰功率的上限值作为发射功率，使得在接收机获得最大输出信噪比，最大程度的干扰接收机的信息接收。将这两种基本方案与文中所提出的干扰机设计方案进行仿真对比。

在路径损耗模型中，信道增益被建模为：$\boldsymbol{h}_{ik}=\sqrt{g_{ik}}\tilde{\boldsymbol{h}}_{ik}$，其中 $i\in\{s,j\},k\in\{d,e\}$，$\tilde{\boldsymbol{h}}_{ik}$ 是服从独立同分布复高斯随机变量，且均值为 0、方差为 1；$g_{ik}=10^{(-\sigma/10)}$ 为衰落路径，$\sigma=30.18+26\log(d_{ik})$ 为路径衰落指数，其中 d_{ik} 为两节点之间的距离。信号噪声功率 σ^2、干扰功率上限值 Q_j 分别为-80dBm 和 30dBm。假设可疑发射机 S、合法窃听节点 E、可疑接收机 D 之间的距离固定为 500 m，S、D、E 的坐标分别为(0, 0) m、(500, 0) m、(0, 500) m。

首先考虑在固定位置上，三种方法的性能对比，干扰机的

空间坐标位置假设为（250，250）m。基于瑞利自由空间衰落模型下，考虑在发射功率 20 dBm～30 dBm 内，将现有的两种基准方法与本文所提的方法进行对比，对比结果由图 2、3 所示。

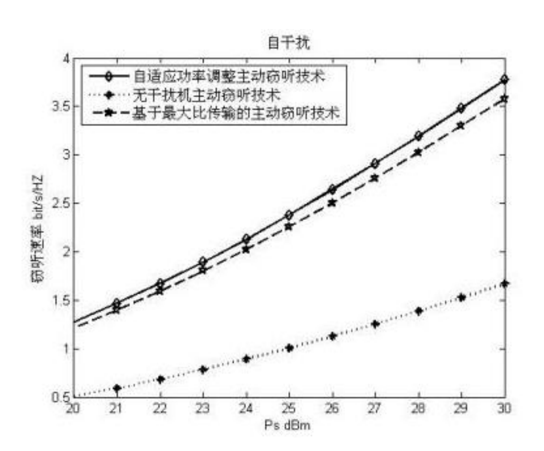


图 2　干扰机位于(250,250)m，存在自干扰时，

窃听速率随发射功率变化的曲线图

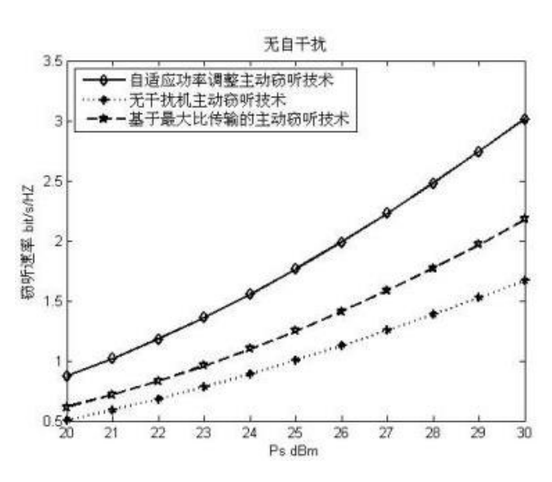


图 3　干扰机位于(250,250)m，无自干扰时，

窃听速率随发射功率变化的曲线图

其次考虑发射功率固定为 25 dBm，干扰机初始位于 S、D 中间位置标记为 q，在水平方向上 100 m～900 m 内，下一点移动位置标记为 j。不同位置下，三种方法的性能比对。结果由图 4、5 所示。

通过图 2、3 可以看出，窃听速率会随着发射功率 P_s 的增加而增加。自适应功率调整方法下，在窃听信道增益较强时，有且干扰功率 $P_j=0$ 作为可行解，即可满足约束条件（窃听速率大于可疑通信速率）；其他情况下，由满足自干扰、无自干扰的判决条件，干扰机通过自适应功率调整，调整干扰机功率 P_j，有干扰功率 $0\le P_j\le Q_j$ 且其平均功率有 $0\le P_{ave}\le Q_j$ 。而基于 MRT 最大比合并方法下，因提高了干扰机的发射功率，使得接收机的噪声功率增加，解调信噪比有所降低，所以系统性能要弱于自适应功率调整策略。无干扰机方法中，根据窃听信道增益与可疑通信信道增益大小关系比较，在窃听信道增益较强时，窃听速率为 0；在可疑信道增益较强时，窃听速率即为：$\frac{P_s\left|\boldsymbol{h}_{sd}\frac{\boldsymbol{h}_{sd}^{H}}{\boldsymbol{h}_{sd}^{H}}\right|^2}{\sigma^2}$ 。因此其平均窃听速率小于 MRT 最大比合并方法。

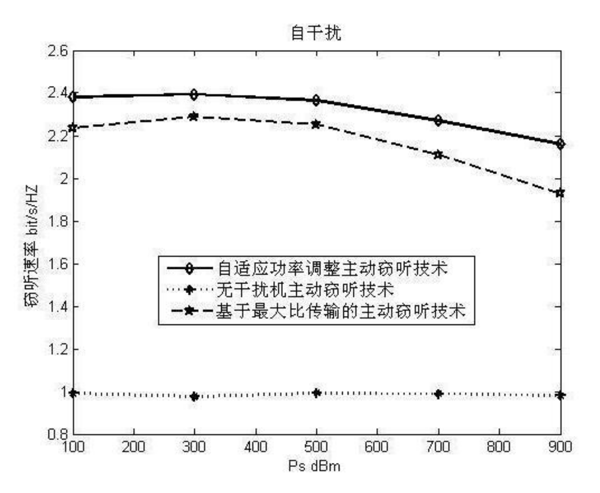


图 4　自干扰情况下，干扰机水平方向上，

100~900m 范围内，三种方法的窃听性能对比结果

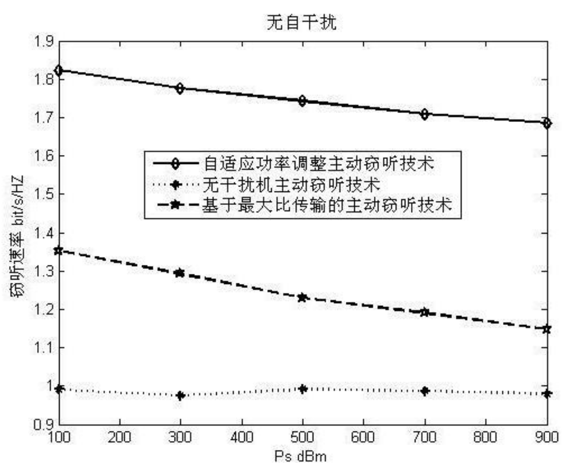


图 5　无自干扰情况下，干扰机水平方向上，

100~900m 范围内，三种方法下窃听性能对比

在图 4、5 中，由于无干扰机方法只与窃听信道增益、可疑通信信道增益有所关联，在干扰机位置改变的时候，对其系统性能影响不大，所以其变化曲线趋于水平。而干扰机位置距离接收机位置越近，两者之间信道增益（$\boldsymbol{h}_{jd}$）越强，接收机干扰功率增强，解调信噪比降低；所以有：干扰机距离接收机越近，窃听速率越强；相反，则越弱。应此对于自适应功率调整方法和最大比合并方法，干扰机位于水平方向上，100~900 m 内，当窃听者靠近可疑接收机：由[0,250] m~[500,250] m 范围内移动时，窃听速率呈递减趋势。窃听者原理可疑接收机：在[500,250] m~[1000,250] m 内时，窃听速率呈递增趋势。因此在实际应用中还需合理设置干扰机的相对位置，以便于获得更好的窃听性能。

综合三种方法比对下，窃听速率的对比结果为：γ_d (无干扰机主动窃听技术)< γ_d (基于最大比传输的主动窃听技术)< γ_d (自适应功率调整主动窃听技术)。

由此可见文中提出的干扰机设计方法所获得的窃听速率性能是优于现有的两种基准方法的。

4 结束语

针对合法窃听技术，分别考虑在有自干扰和无自干扰环境中，合理设置干扰机的相对位置，通过设计最优发射干扰信号，干扰可疑无线链路，改善系统的窃听性能。在不同的应用场景中,干扰机根据功率判断标准，通过自适应功率调整干扰可疑用户之间的通信。仿真可见，干扰机设计方法均取得了比现有的两种基准方法更优的窃听速率性能。

参考文献：

[1] Liang Y, Poor H V, Shamai S. Information theoretic security, foundations and trends in communications and information theory [M]. [S. l.] : Now Publishers Inc, 2009.

[2] Massey J L. An introduction to contemporary cryptology [J]. Proceedings of the IEEE, 1988, 76 (5): 533-549.

[3] Shannon C E. Communications theory of secrecy systems [J]. The Bell System Technical Journal, 1949, 28 (4): 656-715.

[4] Zhang Guangchi, Li Xueyi, Cui Miao, et al. Signal and artificial noise beamforming for secure simultaneous wireless information and power transfer multiple-input multiple-output relaying systems [J]. IET Communications, 2016, 10 (7): 796-804.

[5] Zappone A, Lin P H, Jorswieck E. Energy efficiency of confidential multi-antenna systems with artificial noise and statistical CSI [J]. IEEE Journal of Selected Topics in Signal Processing, 2016, 10 (8): 1462-1477.

[6] Goel S, Negi R. Guaranteeing secrecy using artificial noise [J]. IEEE Trans Wireless Communication, 2008, 7 (6): 2180-2189.

[7] Xu Jie, Duan Lingjie, Zhang Rui. Proactive eavesdropping via jamming for rate maximization over rayleigh fading channels [J]. IEEE Wireless Communications letters, 2016, 5 (1): 80-83.

[8] Zheng Yong, Zhang Rui. Active eavesdropping via spoofing relay attack [C]// Proc of IEEE International Conference on Acoustics, Speech and Signal Processing. 2016: 2159-2163.

[9] Zeng Yong, Zhang Rui. Wireless Information Surveillance via proactive eavesdropping with spoofing relay [J]. IEEE Journal of Selected Topics in Signal Processing, 2016, 10 (8): 1449-1461.

[10] Kapetanovic D, Zheng Gan, Rusek F. Physical layer security for massive MIMO: an overview on passive eaves-dropping and active attacks [J]. IEEE Communication Magzine, 2015, 53 (6): 21-27.

[11] Chi C Y, Li W C, Lin C H. Convex optimization for signal processing and communications from fundamentals to application [M]. [S. l.] : CRC Press, 2017.

[12] Huang Jianli, Li Quanzhong, Zhang Qi, eg al. Relay beamforming for amplify-and-forward multi-antenna relay networks with energy harvesting constraint [J]. IEEE Wireless Communication Letters, 2014, 21 (4): 454-458.

[13] Li Quanzhong, Zhang Qi, Feng Renhai, eg al. Optimal relay selection and beamforming in MIMO cognitive multirelay networks [J]. IEEE Communications Letters, 2013, 17 (6): 1188-1191.

[14] Nguyen D H N, Le L B, Le-Ngoc T. Optimal dynamic point selection for power minimization in multiuser downlink CoMP [J]. IEEE Trans on Wireless Communications, 2017, 16 (1): 619-633.

[15] 耿国桐. MIMO 系统中最大比发射和天线选择技术研究 [D]. 北京：北京邮电大学. 2005.

[16] Liu Qian, Li Ming, Kong Xiangwei, eg al. Disrupting MIMO

[17] communication with optimal jamming signal design [J]. IEEE Trans on Wireless Communications, 2015, 14 (10): 5313-5325.